IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Antonio LAIN et al.
Title:	MANAGEMENT OF SECURITY KEY DISTRIBUTION
Appl. No.:	10/629,599
Filing Date:	7/30/2003
Examiner:	Koempel, Thomas Beatrice
Art Unit:	2132
Confirmation No.:	6218

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The following is the Appellants' Appeal Brief under the provisions of 37 C.F.R. 41.37.

1. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P., which is the assignee of record.

2. Evidence Appendix

There are no related evidence that will directly affect, be directly affected by or have a bearing on the present appeal, that are known to Appellants, the Assignee, or the Appellants' patent representative. The Evidence Appendix (Section 10), attached hereto, states "None".

3. Related Appeals and Interferences

There are no related appeals or interferences that will directly affect, be directly affected by or have a bearing on the present appeal, that are known to Appellants, the

Assignee, or the Appellants' patent representative. The Related Proceedings Appendix (Section 11), attached hereto, states "None".

4. Status of Claims

The present appeal is directed to claims 1, 2 and 4-21. A copy of the presently pending claims under rejection are attached herein in the Claims Appendix (Section 12).

5. Status of Amendments

An Amendment and Reply Under 37 C.F.R. 1.116 is being filed concurrently with this Appeal Brief, in order to make minor corrections to certain claims to address certain issues raised in the final Office Action. The scope of these claims is not believed to be materially affected by these amendments.

6. Summary of the Invention

The present invention is directed to a method of managing security keys provided to users of a service. As mentioned on page 1 of the specification, managing the provision and maintenance of security keys to a large group of anonymous subscribers is difficult, whereby when certain subscribers are unsubscribed, this creates the need to invalidate their security keys, and this has to be done without affecting the security keys of others who are still subscribers to a service.

As described on page 2 of the specification, in a preferred embodiment, a policy for issuing and invalidating security keys is based on economic grounds, so that instead of invalidating a key simply on a contractual basis because a subscription has lapsed for example, the cost to the provider of doing so is assessed, and invalidation takes place at an optimized instant in time from the point of view of the provider.

Independent claim 1 recites:

A method of managing security keys provided to users of a service, the method comprising the steps of:

issuing a security key to a first user eligible to receive the service;

monitoring the first user's status to establish whether the first user is eligible to receive the service;

establishing, in accordance with a policy, a first value associated with invalidation of the first user's security key at a particular point in time, and a second value associated with providing the service to an ineligible user at the particular point in time, and if the second value exceeds the first value, invalidating the first user's security key at the particular point in time,

wherein the first user's security key is kept valid if the second value does not exceed the first value, and

wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible.

Support for the "issuing" step may be found, for example, on page 9, lines 33-34 and on page 10, lines 2-5 of the specification.

Support for the "monitoring" step may be found, for example, on page 2, lines 7-8, page 7, lines 25-30 and page 8, lines 1-5 of the specification.

Support for the "establishing" step may be found, for example, on pages 12 through 15 of the specification. In particular, a first value associated with invalidation of a first user's security key is described with respect to the section entitled "Cost of invalidating Lapsed Customer's Key" on pages 14 and 15 of the specification, and a second value associated with providing the service to an ineligible user is described with respect to the section entitled "The cost to the provider of maintaining an unpaid-for service to lapsed subscribers" on pages 12 to 14 of the specification.

Support for the "wherein the first user's security key is kept valid if the second value does not exceed the first value" features may be found, for example, on page 2, lines 14-24 and on pages 12 to 15 of the specification.

Support for the "wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user" features may be found, for example, on page 2, lines 14-17 and pages 12 to 14 (see "Economic Dilution Cost", for example) of the specification.

Independent claim 10 recites:

A method of managing provision of security keys to a plurality of users of a network service, the method comprising the steps of:

generating a plurality of security keys, each of which is related ancestrally to at least one other security key of the plurality of security keys;

issuing security keys to users;

monitoring users' status for continuing eligibility for consumption of the service; and

upon establishing ineligibility of a user, determining upon the basis of a predetermined policy, a value for economic disbenefit to a provider of the service of (a) invalidation of the ineligible user's security key; and (b) provision of service to an ineligible user.

Support for the "generating" step may be found, for example, on page 8, line 32 to page 9, line 5, page 10, lines 22-29 of the specification, and Figures 2 and 4 of the drawings.

Support for the "monitoring" step may be found, for example, on page 2, lines 7-8, page 7, lines 25-30 and page 8, lines 1-5 of the specification.

Support for the "determining" step may be found, for example, on pages 12 through 15 of the specification. In particular, a value corresponding to provision of service to an ineligible user is described with respect to the section entitled "The cost to the provider of maintaining an unpaid-for service to lapsed subscribers" on pages 12 to 14 of the specification, and a value associated with invalidation of the ineligible user's security key is described with respect to the section entitled "Cost of invalidating Lapsed Customer's Key" on pages 14 and 15 of the specification.

7. Issues

The issues on appeal are: (1) whether the Examiner correctly rejected claims 14 and 15 under 35 U.S.C. § 112, 2nd Paragraph as being indefinite, (2) whether the Examiner correctly rejected claims 14 and 15 under 35 U.S.C. § 112, 1st Paragraph as failing to comply with the written description requirement, (3) whether the Examiner correctly rejected claims 1, 4-6, 10-12 and 18-19 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2002/0031230 to Sweet et al. in view of U.S. Patent No. 6,236,971 to Stefik et al.; (4) whether the Examiner correctly rejected claims 2, 8, 9, 13-15, 20 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Sweet in view of Stefik and further in view of

U.S. Patent No. 6,397,329 to Aiello et al; (5) whether the Examiner correctly rejected claims 14 and 15 under 35 U.S.C. § 103(a) as being unpatentable over Sweet in view of Stefik and Aiello et al. and further in view of U.S. Patent No. 5,457,746 to Dolphin; and (6) whether the Examiner correctly rejected claims 16 and 17 under 35 U.S.C. § 103(a) as being unpatentable over Sweet in view of Stefik '971, Stefik '392 and further in view of Aiello et al.

8. Arguments

I. Claim Rejections – 35 U.S.C. § 112, 2nd Paragraph:

In the final Office Action, claims 14 and 15 were rejected under 35 U.S.C. § 112, 2nd Paragraph, as being indefinite, since the phrase "a length of time subscribed to for the service" is allegedly indefinite. Appellants respectfully disagree with this rejection. In particular, the final Office Action asserts that it is unclear whether or not this phrase is meant to cover a forward or a backward looking subscription. In response, it does not matter whether the subscription is forward or backward. That is, if a subscriber subscribes for a one year service that will start a month from now, then "one year" is the length of time subscribed to for the service. If a subscriber subscribes for a new two year service and is half-way into his/her current service (that is, the subscriber started the previous subscription one year ago), then "three years" (the one year remaining one the subscriber's current subscription, plus the two years added to the subscription by the subscriber) is the length of time subscribed to for the service. Thus, irrespective as to when the subscriber started his/her subscription, claims 14 and 15 recite that the subscription duration is what matters.

As such, claims 14 and 15 are not indefinite, and are fully compliant with U.S.C. § 112, 2nd Paragraph.

II. Claim Rejections – 35 U.S.C. § 112, 1st Paragraph:

In the final Office Action, claims 14 and 15 were rejected under 35 U.S.C. § 112, 1st Paragraph, as failing to comply with the written description requirement, for the reasons set forth on page 7 of the final Office Action. By way of an amendment and reply filed concurrently with this Appeal Brief, claims 14 and 15 have been amended to recite a "zeroth" base node, so as to be in accordance with Figure 4 of the drawings (showing the "Gold" node

set and the "Silver" node set only having a zeroth generation root key A0 as a common ancestor.

As such, claims 14 and 15 fully compliant with U.S.C. § 112, 1st Paragraph.

III. Claim Rejections – Prior Art:

A. Independent Claim 1:

In its rejection of independent claim 1, the final Office Action asserts that column 14, lines 34-40 of Stefik "teach the use of a policy using repository security classes which can create and calculate such a value as described above." Appellants respectfully disagree with this assertion. Namely, column 14, lines 34-40 of Stefik merely describes a processor memory that contains software instructions to perform repository functions, and a descriptor tree storage may be stored in a solid state storage, and a clock may be used for metering usage fees for digital works. These passages of Stefik do not come close to teaching or suggesting a policy that provides that a second value is related to an economic penalty associated with provision of a service to an ineligible user, as explicitly recited in claim 1. It appears that the final Office Action is asserting that just because Stefik has the computer resources that are capable of performing the features recited in claim 1, it teaches those features. This is incorrect, since Stefik says nothing about the specific features recited in claim 1.

Therefore, since Sweet et al. does not rectify the above-discussed shortcoming of Stefik (as acknowledged in the Office Action), independent claim 1 is patentable over the combination of Sweet et al. and Stefik.

B. Dependent Claim 5:

With respect to dependent claim 5, the Office Action asserts that column 6, lines 15-30, and column 14, lines 20-25 and 34-40 of Stefik teach the features recited in this claim. Appellants respectfully disagree. Namely, claim 5 recites that the economic penalty associated with provision of service to ineligible users includes a value representative of dilution of economic value to eligible users consequent to provision of the service to ineligible users. Such features are not taught or suggested in the above-cited portions of Stefik. Namely, column 14, lines 34-40 of Stefik is discussed above with respect to the

rejection of claim 1, whereby that portion of Stefik does not come close to teaching or suggesting the diluation of economic value features of claim 5. Column 14, lines 20-25 of Stefik merely describes conventional memory components (ROM, RAM) for performing a repository function, and column 6, lines 15-30 of Stefik merely lists different types of repository transactions, whereby such repository functions and transactions do not come close to teaching or suggesting the dilution of economic value features recited in claim 5.

Accordingly, dependent claim 5 is patentable for these additional reasons, beyond the reasons given above for its base claim 1.

C. Dependent Claim 6:

With respect to dependent claim 6, that claim recites that the economic penalty includes any costs arising from the provision of network and server capacity to ineligible users. Such features are not taught or suggested in the above-cited portions of Stefik, whereby the portions in column 14 of Stefik (lines 20-25 and 34-40) for which claim 6 was rejected have been discussed above with respect to claims 1 and 5, and whereby column 6, lines 15-30 of Stefik merely lists different types of repository transactions, whereby such transactions do not come close to teaching or suggesting the features recited in claim 6.

Accordingly, dependent claim 6 is patentable for these additional reasons, beyond the reasons given above for its base claim 1.

D. Independent Claim 10:

With respect to independent claim 10, that claim recites: upon establishing ineligibility of a user, determining upon the basis of a predetermined policy, a value for economic disbenefit to a provider of the service of (a) invalidation of the ineligible user's security key; and (b) provision of service to an ineligible user. In its rejection of claim 10, the Office Action asserts that the features recited in that claim "map directly onto the ones shown in claim 1 and are rejected under the same premise", but Appellants respectfully disagree, since claim 10 recites different features than the ones recited in claim 1. Namely, claim 10 recites a step of a value of **economic disbenefit** to a provider of a service, based on two

factors as mentioned above (whereby those two factors are not recited in claim 1). In Stefik, column 15, lines 15-25 describe that an inexpensive handheld repository may be used in cases where losses caused by an individual instance of unauthorized copying is insignificant. The determination of where to place a repository for storing copyrighted material, as taught by Stefik, is not related to invalidating (or not) a user's key based on a determination of economic disbenefit to a provider of a service, since no security key invalidation is being performed in the system of Stefik.

Accordingly, since Sweet et al. does not rectify the above-mentioned shortcomings of Stefik (as acknowledged in the final Office Action), independent claim 10 is patentable over the cited art of record.

E. Dependent Claims 14 and 15:

With respect to the rejection of dependent claims 14 and 15, those claims recite features seen best in the "Gold" and "Silver" triangular areas shown in Figure 4 of the drawings, whereby those two subsets of nodes only share a zeroth generation root node A0. In its rejection of claims 14 and 15, the Office Action asserts that column 8, lines 34-44 and the Abstract of Aiello teach the features in which the security keys of the first subsection of the binary tree only share a zeroth generation root key as a common ancestor with the security keys of the second subsection of the binary tree. Appellants respectfully disagree with this assertion. Namely, Aiello teaches a binary tree that is used as a data revocation structure to update unrevoked certificates, whereby the data revocation structure is grouped into sets and subsets of two. Nothing in column 8, lines 34-44 and in the Abstract of Aiello teaches or suggests that the different sets in Aiello's binary tree only share a first generation root key as a common ancestor.

Accordingly, claims 14 and 15 are patentable for these additional reasons, beyond the reasons given above for their respective base claims.

F. Dependent Claims 16 and 17:

Also, the specific costs delineated in dependent claims 16 and 17 are not taught or suggested by the combined teachings of Sweet, Stefik and Aiello. In more detail, the final Office Action asserts that column 5, line 55 to column 7, line 63 of Aiello teaches that a first value is computed by adding a first cost associated with invalidating all security keys of the ineligible users, with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of the ineligible users. Appellants respectfully disagree. Namely, columns 5, 6 and 7 of Aiello describe a public key revocation scheme in which revocation status information is generated for identified sets of keys, whereby a certificate is grouped into sets with other certificates. Nothing in this portion of Aiello teaches or suggests adding a first cost associated with invalidating all security keys of ineligible users with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of ineligible users. If the Examiner is to maintain this rejection, he is respectfully requested to particularly point out where these specific claim features are to be found in columns 5, 6 and 7 of Aiello (since Appellants' representative cannot find anything even remotely teachings these features in these columns of Aiello).

Accordingly, claims 16 and 17 are patentable for these additional reasons, beyond the reasons given above for their respective base claims.

F. Dependent Claims 20 and 21:

With respect to dependent claims 20 and 21, those claims recites features related to costs associated with creating a new binary tree due to too many security keys being invalidated in an existing binary tree, whereby such features are not taught or suggested by the combined teachings of Sweet, Stefik and Aiello. In particular, the final Office Action asserts that columns 5-7 of Aiello teach the features recited in claims 20 and 21, but Appellants respectfully disagree. Namely, columns 5, 6 and 7 of Aiello describe a public key revocation scheme in which revocation status information is generated for identified sets of keys, whereby a certificate is grouped into sets with other certificates. Nothing in this portion

of Aiello teaches or suggests that a second or third cost includes a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys.

Accordingly, claims 20 and 21 are patentable for these additional reasons, beyond the reasons given above for their respective base claims.

IV. Objection to the Claims:

The objections to claims 1, 15 and 21 as made in the final Office Action have been addressed in the minor amendments made to those claims in the Amendment and Reply filed concurrently with this Appeal Brief.

9. Conclusion

In view of above, Appellants respectfully solicit the Honorable Board of Patent Appeals and Interferences to reverse the rejections of the pending claims and pass this application on to allowance.

Respectfully submitted,

Date May 24, 2007

By _____

William T. Ellis
Registration No. 26,874

Phillip J. Articola
Registration No. 38,819

Attorneys for Appellant

10. EVIDENCE APPENDIX

None

11. RELATED PROCEEDINGS APPENDIX

None

12. CLAIMS APPENDIX

LIST OF THE CLAIMS ON APPEAL (with status identifiers, whereby "Currently Amended" signifies amendments made via an Amendment an Reply filed concurrently with this Appeal Brief)

1. (Currently Amended) A method of managing security keys provided to users of a service, the method comprising the steps of:

issuing a security key to a first user eligible to receive the service;

monitoring the first user's status to establish whether the first user is eligible to receive the service;

establishing, in accordance with a policy, a first value associated with invalidation of the first user's security key at a particular point in time, and a second value associated with providing the service to an ineligible user at the particular point in time, and if the second value exceeds the first value, invalidating the first user's security key at the particular point in time,

wherein the first user's security key is kept valid if the second ~~valid~~ value does not exceed the first value, and

wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user.

2. (Previously Presented) A method according to claim 1 wherein the policy further provides that the first value is related to the economic penalty associated with reconfiguration of security keys issued to other users consequent to invalidation of the first user's security key.

3. (Canceled).

4. (Previously Presented) A method according to claim 1 wherein the second value is calculated by aggregating the economic penalty associated with provision of the service to each ineligible user.

5. (Original) A method according to claim 4 wherein the economic penalty associated with provision of service to ineligible users includes a value representative of dilution of economic value to eligible users consequent to provision of the service to ineligible users.

6. (Previously Presented) A method according to claim 1 wherein the economic penalty of providing the service to ineligible users includes any costs arising from the provision of network and server capacity to ineligible users.

7. (Previously Presented) A method according to claim 2 wherein the security keys are generated in an ancestrally-based hierarchy, and wherein invalidation of a given key necessitates a need for reconfiguration of each security key in the hierarchy.

8. (Previously Presented) A method according to claim 7 wherein upon invalidation of a given security key, an other security key requires reconfiguration only to the extent that it shares common ancestor security keys with the given invalidated security key.

9. (Original) A method according to claim 8 wherein the hierarchy is a binary tree.

10. (Currently Amended) A method of managing provision of security keys to a plurality of users of a network service, the method comprising the steps of:

generating a plurality of security keys, each of which is related ancestrally to at least one other security key of the plurality of security keys;

issuing security keys to users;

monitoring users' status for continuing eligibility for consumption of the service; and

upon establishing ineligibility of a user, determining upon the basis of a predetermined policy, a value for economic disbenefit to a provider of the service of (a) invalidation of the ineligible user's security key; and (b) provision of service to an ineligible user.

11. (Previously Presented) A method according to claim 10 further comprising the step of invalidating the security key if the disbenefit of providing service to an ineligible user is greater than the disbenefit of invalidating the security key.

12. (Previously Presented) A method according to claim 11 further comprising the step of aggregating the disbenefit of providing the service to each ineligible user, and invalidating the security key only if the aggregated disbenefit of providing the service to all ineligible users is greater than the disbenefit of invalidating the security key.

13. (Previously Presented) A method according to claim 10 wherein invalidation of the security key necessitates reconfiguration of each other security key to the extent another security key shares common ancestry with the invalidated security key.

14. (Currently Amended) A method according to claim 9, further comprising the step of:

assigning security keys to users based on a length of time subscribed to for the service,

wherein a first set of users who have subscribed for a length of time less than a predetermined time are assigned security keys in a first subsection of the binary tree,

wherein a second set of users who have subscribed for a length of time greater than or equal to the predetermined time are assigned security keys in a second subsection of the binary tree, and

wherein the security keys of the first subsection of the binary tree only share a ~~first~~ zeroth generation root key as a common ancestor with the security keys of the second subsection of the binary tree.

15. (Currently Amended) A method according to claim 13, wherein the related ancestry of the security keys is determined by way of a binary tree in which the security keys are assigned,

wherein the issuing step ~~comprising~~ comprises the step of:

assigning security keys to the users based on a length of time subscribed to for the service,

wherein a first set of users who have subscribed for a length of time less than a predetermined time are assigned security keys in a first subsection of the binary tree,

wherein a second set of users who have subscribed for a length of time greater than or equal to the predetermined time are assigned security keys in a second subsection of the binary tree, and

wherein the security keys of the first subsection of the binary tree only share a ~~first~~ zeroth generation root key as a common ancestor with the security keys of the second subsection of the binary tree.

16. (Previously Presented) A method according to claim 4, wherein the security keys are generated in an ancestry-based, binary tree hierarchy,

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy,

wherein the first value is computed by adding a first cost associated with invalidating all security keys of the ineligible users, with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of the ineligible users.

17. (Previously Presented) A method according to claim 10, wherein the security keys are generated in an ancestry-based, binary tree hierarchy,

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy,

wherein the value for economic disbenefit to the provider is computed by adding a first cost associated with invalidating the ineligible user's security key, with a second cost associated with reconfiguring all security keys of eligible users that are in an upper ancestry level in a same ancestry chain as the ineligible user's security key, and with a third cost associated with invalidating all security keys in the binary tree hierarchy that are of a lower ancestry level in the same ancestry chain as the ineligible user's security key.

18. (Previously Presented) A method according to claim 1, wherein the issuing step is performed by a server, and wherein the issuing step includes providing the

security key to the first user in a cookie returned to the first user by the server over the Internet.

19. (Previously Presented) A method according to claim 10, wherein the issuing step is performed by a server, and wherein the issuing step includes providing the security keys to the users in cookies respectively returned to the users by the server over the Internet.

20. (Previously Presented) A method according to claim 17, wherein the second cost includes a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys.

21. (Currently Amended) A method according to claim [[18]] 17, wherein the third cost includes a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys.